REMARKS

The specification has been corrected in the same manner as was done in the parent application, and now comports with what is shown in Figure 1C of the application.

Claims 1- 33 have been canceled. Claim 34-45 have been added. The added claims are substantially directed to the subject matter of claim 12 of the application as originally filed.

The invention provides the ability to verify that certain events have occurred by transmission of a digital signature and encrypted data to a data acquisition system. This, in effect, leaves an electronic fingerprint which can be verified and authenticated. As shown in Figure 1A, and discussed in the application on pages 5 and 6, a smart card can be used in the practice of this invention, and can be maintained in a tamper proof housing 106. The smart card can be connected to or have on board one or more sensors 105. The smart card would include a memory 103, processing units 104, and an encryption module 107. The smart card is connected to a receiver 110 and transmitter 120. As explained on page 6 of the application, these components 110 and 120 may be integrated onto the card or be discrete components. Also it should be clear that one device (e.g., a transceiver) might be used as both a receiver 110 and a transmitter 120. Figures 1b and 1c show use of the device of this invention with transmitters and receivers at remote locations such as a road side station, a traffic light, or another identical device.

The text on page 6, lines 1-2, discuss disabling the vehicle when tampering is detected. The text on pages 8 and 9 of the application discuss having, for example, a truck with one of the devices, stopping transmission upon of the signature data upon detecting tampering of the event recorder, cargo or lock. In this instance, for example, a truck that is not transmitting a signal may be subject to manual inspection. Claim 12 as originally filed, discusses transmitting the signature data upon the occurrences of an event (i.e., tampering with locks or the event recorder. A practical example of the technology could the situation where cargo loaded on boat bound for the Port of Baltimore is tampered with en route, such as might occur if a terrorist cell intends to illegally important weapons or the like, the sensor would transmit the vehicle signature data (i.e., the boat and cargo container) upon the occurrence of tampering such that Customs Officials could readily know in advance to search the vessel upon its arrival. Likewise, as another example, tampering with the vehicle locking mechanisms of a car could result in transmitting the vehicle signature data to the police to alert the police of the possible theft of the vehicle.

Respectfully submitted,

Michael E Whitham
Reg. No. 32,635

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557